TEACHING CYBERCRIME IN THE POST GRADUATE BAR COURSE IN UGANDA

Dr. Maureen Owor

Abstract

This paper supports the teaching of cybercrime in the Law Development Centre's post-graduate Bar course, because cybercrime is a nascent area with international dimensions of which empirical evidence exists. Furthermore, on February14, 2011, Uganda enacted its first cybercrime legislation- the Computer Misuse Act 2011. The paper aims to stimulate debate on the effectiveness of the Act in dealing with terrorist acts that are perpetuated by use of computers. An e-mail allegedly linked to the mastermind(s) of the July 11, 2010 deadly bombings in Kampala, provides a lens through which two aspects of the Computer Misuse Act are examined namely: the narrow definition of computer misuse; and the inadequate provisions on proportionality and human rights, and judicial oversight in the procedural framework. Such an e-mail is a learning material well suited for the problem-based learning methods applied during the Bar Course. By way of concluding reflection, the author highlights research and training, as a means by which legal solutions to the lacunae in the legislation may be found.

Key words: Teaching, Cybercrime, bar course

Introduction

This article is a revised version of a presentation: "Legal perspective on Cybercrime in Uganda" delivered by the author on August 27, 2010 at a workshop on Identity Theft Sensitisation and the launch of the African Centre on Cyber law and Cybercrime Prevention organised by UNAFRI in Kampala, Uganda.

In June 2010, the Law Development Centre (LDC) held a workshop (4th - 7th June 2010) on curriculum review of subjects taught on the post-graduate Diploma in Legal Practice, also called the 'Bar Course'.[3] During deliberations, the teaching of cybercrime in the Criminal Proceedings course was raised by lecturers. The law teachers were in agreement that Criminal Proceedings should incorporate cybercrime --- an area of topical interest. The academics also underscored the importance of training lecturers in this area, and conducting research into such contemporary legislation by the Department of Research, Law Reform and Publications.

In the following month, on July 11, 2010, bombs exploded at two venues on the outskirts of the capital Kampala, killing at least 76 people, injuring many more and destroying property. Members of the Al-Shabaab

3 LDC is the only institution in Uganda accredited by law to conduct courses for the Post Graduate Diploma in Legal Practice. The diploma is a pre-requisite to practising in the courts of law in Uganda.

terrorist group from Somalia claimed responsibility. Later, on August 4, 2010, Parliament passed the Computer Misuse Bill (No. 23 of 2008). This piece of legislation - the first of its kind in Uganda - was aimed at tackling cybercrime. According to the then Minister for Information and Communication Technology, Aggrey Awori, the move by Parliament to debate the Bill, was given momentum by the July 11 bomb blasts in Kampala (*New Vision* 3rd August, 2010). The Computer Misuse Act (No 2 of 2011), hereafter referred to "CMA", became law in 2011, the first of three laws drafted by the Uganda Law Reform Commission (ULRC) to deal with computer and other e-crimes. The other two Acts passed by Parliament are the Electronic Signatures Act (No. 7/ 2011) and the Electronic Transactions Act (No 8/2011).

Coincidentally, on 26th August 2010, the Africa Centre for Cyberlaw and Cybercrime Prevention (ACCP) was launched at the United Nations African Institute for the Prevention of Crime and Treatment of Offenders (UNAFRI) in Kampala. During the launch, academics from Makerere University, Nkumba University, Kampala International University and Uganda Christian University, made it clear that their Law Schools did not teach cybercrime within the criminal law course. This is not surprising given firstly that these three bills had only just been passed at the time, and secondly that there is no specific Ugandan law as yet on cybercrime. A question arose: should LDC cover cybercrime if it is not taught in Law Schools? Participants reasoned, correctly in my view, that if LDC covered areas like cybercrime that are not taught at undergraduate level, the Bar Course students would be at a disadvantage because they would have no prior knowledge of the topic more so if there was no legislation proscribing cybercrime. Participants concluded that cybercrime could be covered at LDC only *after* universities teach it. Even so, cybercrime would not be taught as a compulsory course unit at *all* the universities.[4] Although we shall come back to this point later, let us examine three reasons why LDC should teach cybercrime in Criminal Proceedings against this backdrop.

Firstly, cybercrime is an embryonic area of criminal practice in Uganda but with international dimensions. Dr. Masamba Sita, Director of UNAFRI, explains that although Africa accounts for only 85 million of the 1.8 billion users of the internet, it has a tremendous increase of 1,800% in users over the past decade. In his view:

> (...) Africa has a stake in the global fight against cybercrime, because cybercrime itself is borderless and nationless. Cybercrime pays no heed where perpetrators, victims or authorities are physically located. (...) A criminal may cross an ocean, violate a dozen laws of a dozen nations, and then vanish all in an instant. Thus, we must fight cybercrime by ensuring that our work crosses oceans and nations, and developing global cooperation and practices that keep us a step ahead of criminals." (2010)

4 For admittance on the Bar course, an eligible student must have passed Legal Methods, Constitutional law, Contract, Criminal Law, Torts, Evidence, Civil Procedure and Criminal Procedure, at the undergraduate law level: (*The Advocates (Professional Requirements for Admission to Post Graduate Bar Course,* Paragraph 4 (2) and Schedule 1).

This excerpt highlights the international dimension of cybercrime and the importance of espousing a multi-faceted approach in developing a legal framework to handle cybercrime. In proposing national and international mechanisms for combating cybercrime, Schjølberg and Ghernaouti-Hélie argue that: "An adapted legal framework and laws that are applicable to the digital world must be operational at the national level and internationally compatible" (2009, 10). This quote shows that national legal frameworks must fit into an international milieu given the borderless nature of cybercrime.

Secondly, empirical evidence exists of the prevalence of cybercrime. Chawki and Okike (2009, 149-156), citing data from the Computer Security Institute, demonstrate the scale of the problem internationally. Their findings show that 64.3% of 6,100 respondents experienced malware infection in 2009 compared to 50% in 2008. While the number of victims is on the increase, countries are also fast enacting legislation to deal with cyber criminals. Comparatively, Tushabe and Baryamureeba (2005 p. 68-69) in their study on the incidence of cybercrime in Uganda established that 95% of the 500 study subjects (Internet users) were victims of cybercrime. Spam and virus attacks were cited as the most common problem. The authors concluded that victims do not report these incidents to the police or relevant authorities, due in part to the lack of a legal framework.

Thirdly, Uganda has now put in place legislation to combat cybercrime comprising the three Acts mentioned previously; the Electronics Transactions Act, the Electronic Signatures Act and the CMA. This article will, however, focus on the CMA. The CMA was passed by the Parliament of Uganda on August 4, 2010. The date of assent by the President was November 1, 2010 and the CMA was gazetted on the February 14, 2011. The date of commencement of the CMA appointed by the Minister for Information and Communication Technology is April 15, 2011. The CMA is intended, among other things, to prevent the misuse of information systems including computers. In that regard, Part IV CMA creates thirteen offences as follows: Unauthorised access (Section 12), Access with intent to commit or facilitate commission of an offence (Section 13), Unauthorised modification of computer material (Section 14), Unauthorised interception of computer service (Section 15), Unauthorised obstruction of use of computer (Section 16), Unauthorised disclosure of access code (Section 17), Unauthorised disclosure of information (Section 18), Electronic fraud (Section 19), Offences of abating and attempting to commit an offence under the Act (Section 21), Child pornography (Section 23), Cyber harassment (Section 24), Offensive Communication (Section 25) and Cyber stalking (Section 26).

From the foregoing discussion, these three reasons justify why LDC ought to cover cybercrime in future. Moreover, LDC's mission statement is "To develop legal capacity in Uganda". Developing such competence among students on the Bar Course includes creating a curriculum that covers topics like cybercrime that are of international relevance given their borderless nature. Even so, as this paper demonstrates, the CMA's substantive and procedural framework may not adequately

deal with criminal conduct of a terrorist nature committed in cyberspace. Take the example of the tragic events of Sunday July 11, 2010 outlined previously. Of relevance to our discussion are the ensuing police investigations that uncovered an e-mail purportedly connecting a Pakistani national to the Al-Shabaab terrorist group (*New Vision 19 July* 2010, p.2). This e-mail can be used as a hypothetical case study of a heinous crime that ostensibly involves the use of computers. This is because there is some evidence that the email may be inextricably linked to the bombings and the subsequent loss of life, destruction of property and injury to persons.

Using the example of the 'Al-Shabaab e-mail', this paper illustrates that the CMA has a narrow definition of computer misuse that excludes terrorist acts; and a procedural framework that does not sufficiently cover principles of proportionality, human rights, and judicial oversight. To address these concerns, the paper is set out in three sections. First is a background to teaching methods on the Bar course. Next is the main discussion in which the substantive and procedural complexities of the CMA are analysed using a problem-based learning approach. In conclusion, the author proposes research and training as solutions to rectifying the legal challenges posed by the CMA.

An overview of teaching methods on the bar

The Bar course at LDC covers two broad areas: the knowledge areas and the skills area. The knowledge area comprises core subjects that include Criminal Proceedings. The other subjects are Civil Proceedings, Commercial Transactions, Land Transactions and Domestic Relations. The skills area imparts to students: advocacy skills (court appearances), conference skills (interviewing clients), drafting (General written skills), legal research skills, opinion writing (giving written advice) and resolution of disputes out of court. For knowledge and skills areas, LDC uses four methods of instruction: 'self-paced learning', problem-based learning, trial simulations and lectures.

Self-paced learning is where students conduct individual research into the relevant laws, procedure and jurisprudence, and then apply the knowledge acquired to solve a real or hypothetical case. Self-paced learning is supplemented by the other three modes of instruction: problem-based learning, trial simulations and lectures by guest speakers. Problem-based learning is through case studies (called 'case files' or 'problem questions') constructed around on-going police investigations, or real life court cases. The case files are modified to take into consideration changes in the law, policy or related factors. The trial simulations take the form of mock trials in which the students act as prosecutors, defence attorneys, witnesses, court clerks and (sometimes) judges. Problem-based learning and moots are augmented with talks by guest speakers, comprising eminent lawyers working in Uganda Police Force, the Judiciary, the Directorate of Public Prosecutions, private legal practice and organisations. The recurrent theme in these approaches is the

use of current events reported in the press; court cases that are listed for hearing; and cases that are being tried or have been concluded in the courts of law.

Problem-based learning is a suitable tool through which we can appraise the CMA. This is because case files avail an opportunity for an in-depth critique of the law by the students. In problem based learning, students in their simulated 'law firms' discuss a case file with their professional advisors (lecturers). Discussions in Criminal Proceedings typically cover offences under substantive law and the procedural framework within which law enforcement agencies, like the police, operate (*LDC Prospectus 2009-2010*: para 2.2, pp. 43-46).

In investigating the substantive law and the procedural framework of the CMA, we shall use the example of the 'Al Shabaab e-mail' outlined above, while taking into account the fact that police investigations are not yet complete. Furthermore, the CMA is now law as its commencement date was April 15, 2011. For that reason, our critique will investigate the doctrine of legality under Article 23 (7) and (12) of the Constitution of Uganda, that prevents the Pakistani suspect in this case from being tried under a law (CMA) that was not in force at the time of the commission of the offence. Such adaptation is appropriate as it reflects the manner in which LDC case files are tailored by the Bar Course Advisory Board (that moderates all teaching content) to cover varied legal situations.

Legal complexities in the computer misuse act

The 'firm' discussions characteristically commence, by way of introduction, with a recapitulation of substantive law and key elements of procedural law, to establish existing knowledge on the part of the students. This recap is premised on the fact that students have studied the theoretical framework, historical, political and socio-economic background, substantive and procedural criminal law during their undergraduate law degree.

As we have discussed previously, in teaching cybercrime it is likely that a significant number of the students may not have studied cybercrime for their undergraduate law degrees. That being the case, the discussions would begin with an introduction to cybercrime by the professional advisor. The introduction would be augmented by a guest speaker who would give a 1-hour lecture on the substantive law.

The starting point will be an overview of Uganda's legislation on cybercrime, dispersed in three Acts: the CMA, the Electronic Transactions Act 2011 and the Electronic Signatures Act, 2011 afore-stated. There is no specific law on cybercrime i.e. 'Cybercrime' Act. Nonetheless, students would be introduced to the background to the CMA found in the Uganda Law Reform Commission's (ULRC) *A study on Electronic Transactions Law* (2006, Chapter5"Computer Crime"). There are also international conventions like the United Nations *Convention against Transnational Organised Crime* (2000); and regional mechanisms like the Council of Europe's

Convention on Cybercrime (2001) (hereafter "CECC") and the *Convention on the prevention of Terrorism* (2005) (hereafter "COPT"). At the regional level, in Africa, there is the newly-created ACCP that aims to fight cybercrime at all levels. The class would also be made aware of developments at the sub-regional level, namely the proposal by the five East African Community member states (Kenya, Tanzania, Uganda, Burundi and Rwanda) to set up Computer Emergency Response Teams to fight cybercrime, and to reconcile the laws of these countries (Kisambira, 2010). This merger of cybercrime laws is the initiative of the East African Communications Organisation.

Students will take note of the International Telecommunications Union (ITU) toolkit for cybercrime legislation. This draft toolkit (February 2010) developed by the American Bar Association, aims to provide sample legislative language and reference materials that may assist countries to set up synchronised cybercrime laws and procedural rules. Given this outline, the class will be better equipped to examine the substantive legislation, specifically the definitions of computer misuse in the CMA.

1. *Substantive legislation- narrow definitions of cybercrime*

In discussing case files, students are expected to define offences and apply the facts of a case to the elements of the offence. In our hypothetical case file, the issue for consideration is whether the generation of the 'Al-Shabaab e-mail' and its contents disclose any offence under Part IV CMA previously discussed. Let us postulate that the ongoing police investigations into the 'Al-Shabaab e-mail' reveal that the Pakistani suspect had unauthorised access to a computer to facilitate an act of terrorism by sending the 'Al Shabaab e-mail'. Such email could be for the purpose of making plans for terrorist activities, for informing terrorists, or even for recruiting or training terrorists (online). The students would have to evaluate whether these acts contravene the provisions in Part IV of the CMA.

A close inspection of Part IV CMA reveals no offence of unauthorised access to computers for terrorism activities. In our hypothetical situation, it appears that no offence is committed under this Act. Rather, the CMA introduces offences specific to the penetration, interception, modification and obstruction to computer systems. There is also a range of offences mentioned above that criminalise acts of cyber harassment, cyber stalking, child pornography and offensive communication using a computer. This lacuna may arise because the CMA is modelled largely on the Singapore Computer Misuse Act Cap 50 (1993) and the United Kingdom Computer Misuse Act 1990 (ULRC Report 2006, Para 5.8.3 and Recommendations 20 and 21). Yet, offences proscribed in these two Acts are grounded on criminal cyber conducts in the 1990s and, therefore, have no offences on terrorist acts in cyberspace using computers.

To the contrary, the ITU toolkit gives examples of offences that could be created.

For instance, Section 2 (d) of the ITU toolkit legislation prohibits *Unauthorised Access (to computers, computer systems and networks) for Purposes of Terrorism*. The section criminalises unauthorised access intended to develop, formulate, plan, facilitate, assist, inform, conspire or commit acts of terrorism but is not limited to acts of cyber terrorism. These terms are defined further in Paragraph 4. 2. The ITU toolkit also usefully sets out the offence of *Unauthorised Access to or Acquisition of Computer Programme or Data for Purposes of Terrorism* under Section 3 (f). It is noteworthy that the ITU toolkit is based largely on the CECC though with modifications.

Relevant guidance may also be sought from COPT. Schjølberg and Ghernaouti-Hélie suggest that countries could use COPT as a guide to draft offences on the prevention of terrorist use of the Internet. (2009, pp 4-5). In their discussion of COPT, Schjølberg and Ghernaouti-Hélie explain that terrorist attacks in cyberspace are a category of cybercrime. The term "cyber terrorism" is often used to describe incidents where a criminal act is perpetrated by the use of computers resulting in violence, destruction or disruption of services. The aim is to create fear by causing uncertainty in a population, with the purpose of influencing a government or population to conform to a particular political, social or ideological agenda (2009, pp 54-57). As Clive Walker points out, there is a distinction between those who use the Internet in a secondary role to further terrorism (such as in our hypothetical case) and those who use the Internet as the object or mode of attack. (2006:633)

Extrapolating these definitions to the CMA, a close scrutiny of Part IV on Offences shows that it neither proscribes the criminal misuse of computers to further acts of terrorism; nor prohibits terrorist attacks in cyberspace. Instead, a possible offence in relation to our hypothetical case is in Section 15 (1) (c) that criminalises acts of any person who uses or causes to be used, a computer or any other device for the purpose of committing an offence under paragraph (a) or (b). Of relevance is paragraph (a) that creates an offence for a person to access any computer without authority for the purpose of obtaining any computer service. However, computer service as defined in Section 2 does not include sending an e-mail. Rather, computer service covers computer time, data processing and storage retrieval of data.

Additionally, unauthorised access is not defined in the interpretation section (Section 2). Instead, the CMA creates offences in Section 12 (1) and (2) that punish the intentional access, interception or interference with a programme or data "without authority or permission". To better understand this Section, one may turn to the definition of "authorised access" in Section 5. This section introduces in concise terms, the concept of entitlement of a person to control access to a programme or data and the giving of consent to a person to gain entry to a programme or data in question. Read together, Sections 5 and 12 imply that the perpetrator should have had no entitlement or explicit consent to access that programme or data on the computer at the time of the commission of the offence (unauthorised access).

The class would then examine case law that defines unauthorised access in computer misuse offences. Since jurisprudence in this area is yet to develop in Uganda, the students would study decisions from jurisdictions with an older established legal framework on cybercrime like the United Kingdom. There the courts have grappled with the meaning of unauthorised access in computer misuse offences in the Computer Misuse Act 1990.

Take the case of *DPP v Bignell [1998]*. There a police officer used the police national computer system to identify the owner of a car of his ex-wife for his own use. He was charged under the United Kingdom Misuse of Computers Act 1990. The court held that the Act was meant primarily to protect computers, not the information held. Therefore Bignell could not be found guilty as his actions were not within the definition of "unauthorised access" under the Misuse of Computers Act.

The case of Bignell was later overturned in *Regina v Bow Street Magistrates Court and Allison* [1999]. The facts are that the ordinary work of the defendant (Allison) was to access parts of a database to supply information about credit card accounts. His co-defendant asked him to obtain similar details from other areas of the database so as to assist her to commit a fraud. The question was whether, if he had authority to access part of the database, he could be unauthorised to access other parts of the database. The House of Lords declined to follow the earlier case of *DPP v Bignell* which it decided was no longer good law. Their Lordships then expounded on the meaning of Section 17(5) of the Computer Misuse Act which provides that:

> "Access of any kind by any person to any programme or data held in a computer is unauthorised if -
> (a) he is not himself entitled to control access of the kind in question to the programme or data; and
> (b) he does not have consent to access by him of the kind in question to the programme or data from any person who is so entitled."

The court determined that Section 17(5) is an interpretation section whose subsection lays down two conditions of lack of authority.

> "The first is the requirement that the relevant person be not the person entitled to control the relevant kind of access. The word "control" in this context clearly means authorise and forbid. If the relevant person is so entitled, then it would be unrealistic to treat his access as being unauthorised. The second is that the relevant person does not have the consent to secure the relevant kind of access from a person entitled to control, *i.e.* authorise, that access."

This extract explains clearly, the meaning of unauthorised access. The court further found that there was no concept, within Section 17 (5) that defines the

meaning of authority to access (for purposes of the Act), which could broaden the authority to allow access parts of a database to all comparable kinds of data within a database. Since such a concept was not present in the Act, the House of Lords held that although Allison was authorised to access some information, he did not have authorisation to access the relevant information. This effectively overturned the decision in *Bignell.*

The decision in *R v Bow Street Magistrates* though not binding on Ugandan courts, is nevertheless highly persuasive as it gives a concise explanation of unauthorised access and how it may be construed. Applying this reasoning to our hypothetical case, the class will appreciate the complexities that arise in attempting to apply the provisions in Sections 5 and 12 of CMA in the absence of an interpretation section on unauthorised access. Also, the CMA does not cover unauthorised access to computers in an ancillary role to further terrorism or for terrorist attacks on the Internet as suggested in the ITU toolkit. Even if one argues that wider interpretation could be given to these sections to cover such acts of terrorism, there still remains the issue of whether the CMA can be applied retrospectively under the principal of legality.

The class will explore the principle of legality enshrined in Article 28 (7) which provides that no person shall be charged or convicted of a criminal offence founded on an act (or omission that did not constitute an offence at the time that act took place. Since the CMA commenced on the April 15, 2011 (Instrument 35 of 2011) and the e-mail was discovered the previous year between June and August 2010, the class should understand that under the principle of legality the Pakistani national cannot be charged under the CMA because the Act was not law at the time the offence was allegedly committed. Such a charge would be outside the scope of Article 28 (7) of the Constitution and a fundamental breach of a suspect's right to a fair trial. In this context, the decision in *R v Robert & Another* [1969] is instructive. The facts are that the accused were charged with and convicted (on their own pleas of guilt) of being in possession of *moshi* (liquor) without a licence contrary to the Moshi (Manufacture and Distillation) Act 1966 of Tanzania. The Act, however, had not yet come into force as required, by notice in the gazette. The question for determination on revision was whether the conviction could be sustained. The court held that the proceedings were a nullity because the Act under which the accused were charged and convicted was not yet law. The class would note that though this Tanzanian case is of persuasive authority in Uganda, it nonetheless underscores the principle of legality.

In light of these legal complexities, the class would investigate the possibility of charging the suspect (in our hypothetical case) instead under provisions of existing national law specifically the Anti-Terrorism Act (ATA) 2002. Given that the evidence in our hypothetical case is that of an e-mail purportedly linking the suspect to the Al-Shabaab terrorist group that carried out the bombings, then the most appropriate section would be Section 7 (2) (b). This section makes it an offence for any person

who for purposes of influencing the government or (among others) intimidating the public and for a political, religious or other aim, has direct involvement or complicity in the attack on a group of persons in public institutions. The case will revolve on whether the e-mail shows *complicity* on the part of the suspect in the July 11, 2010 deadly attacks in Kampala. In this regard, the ATA under Section 19 (5) (b), permits an authorised officer to intercept e-mails made, issued or received during the course of investigations. If the officer can show that the contents of the e-mail link the suspect to the bomb attacks, then the charges could be brought under the ATA. Still, students will note that the ATA does not directly penalise criminal acts of a terrorist nature involving the misuse of computers, since the ATA precedes the CMA having been passed in 2002.

2. *Procedural issues- Proportionality and human rights and judicial oversight*

The class discussion would then turn to the procedural framework of the CMA. Criminal proceedings commence with an appraisal of police investigative procedure like the conduct of searches, seizures and arrests of suspects. Notably, the investigative procedures set out in the CMA under Part IV relate only to searches and seizures. Searches with a warrant are provided for under Section 28(1) (3) (4) (5). Data may be seized under Section 28 (2) (3) (6) and (8).

A closer examination of the CMA shows key areas that are not covered, namely the principle of proportionality and human rights, and judicial oversight - all essential aspects of the procedural framework. Proportionality has two related definitions. First, proportionality means the impact of procedural powers by law enforcement agents upon the rights, responsibilities, and legitimate interests of third parties alien to the facts investigated shall be considered when conducting such investigations (ITU toolkit: Paragraph 13 and Part 4 Explanatory Comments to Sample Legislative Language at 35). Secondly, Schjølberg and Ghernaouti-Hélie argue that procedural elements should include measures that preserve fundamental human rights including privacy. Also, investigations (among other areas) must be based on the rule of law, and be under judicial control (2009, pp. 15-16). In sum, proportionality in cybercrime legislation means that procedural powers of law enforcement agencies must be exercised within the context of human rights and judicial oversight.

Scholars will examine the fundamental human rights that must be protected during a search and seizure by the police: called an authorised officer in the CMA. The only provision on protection of rights is in Section 28 (6) CMA where in seizing or taking samples of data, with or without a warrant, an authorised officer shall have regard to rights and interests of a person affected by the seizure to carry on normal activities. At first glance, the rights of suspects and the rights of third parties appear to be protected. On closer scrutiny, it is not clear *which* rights are protected. For instance, there is no mention in Section 28(6) of the protection

of the right to privacy enshrined in Article 27 of the Uganda Constitution. Article 27(1) proscribes an unlawful search of the person, home or other property of a person; and Article 27(2) forbids the interference with the privacy of a person's home, correspondence, communication or other property.

Protection of privacy is crucial in order that procedural powers of investigation do not impact negatively on legitimate interests of suspects or third parties during investigations. Any violation of the right to privacy must be justified if investigations are within the line of prosecution. As Senyonjo explains, legitimate interference with the right to privacy may occur due to national security or public safety, and if such interference is necessary in a democratic society. This necessity depends on whether there is a pressing social need for the interference. (2002-2003, pp. 56, 61-64). Under Article 43 of Uganda's Constitution, the right to privacy is balanced against the need for necessity. This is because the right to privacy is not one of the rights and freedoms delineated in Article 44 (a)-(d) from which no derogation is permitted. These are: freedom from torture, cruel, inhuman or degrading treatment, slavery or servitude; the right to a fair trial and to an order of habeas corpus. Even so, any subsequent retention of information gathered during investigations or disclosure of such information to the public may constitute a violation if these actions are not justified (Senyonjo: 56). This means that private information or data regarding third parties on a computer or electronic record should not be released to the public, if it has no bearing on the investigations.

One may argue that for the issuance of warrants for all searches and seizures under Section 28 of the CMA, one protects procedural rights of suspects and third parties. As Senyonjo argues citing the European Court of Human Rights decision of *Funke v France* (A256-A (1993) at para 57), prior judicial authorisation for search warrants is an imperative in order to accomplish proportionality of police aims (2002-2003, p 64). Arguably, Section 28 of the CMA should be read in conjunction with the Police Act that provides some guidance on protection of rights during searches. For instance, Section 27(9) provides that the search shall be conducted in "a humane manner and unnecessary damage or destruction to property shall be avoided". This means that the provisions of the Police Act enjoin officers to conduct a search without subjecting a person to cruel, inhuman or degrading treatment forbidden by Article 24 of the Constitution. Other safeguards include: the recording of the grounds for conducting a search and the item being sought (Section 27 (1) and (3)) and a copy of the record shall be given to the magistrate and the owner of the premises (Section 27(5)). Under Section 27(6), the occupant of the place searched or some other person on their behalf "shall in every instance be permitted to attend during the search; and where possible a local leader should be present during the search." Thus, friends, relatives, neighbours, even Local Council officials may be present during the search.

In relation to seizures, Section 29(2) Police Act provides that the officer shall record the seizure and description of property seized. That record should be signed by

the officer and occupant of premises. A more general provision is in Rule 2 (b) of the Disciplinary Code of Conduct for Police Officers (Schedule to Police Act as amended by Act 16 of 2006), wherein police officers may not take away any rights of any person without any reasonable cause. Even though what is reasonable is not defined in the Code, I suggest that reasonable cause means the police officer should have sufficient trustworthy facts or circumstance that justifies their belief that an individual's rights should be infringed. Such circumstances could include national security, public safety or a social need for the interference (vide our foregoing discussion). Accordingly, Rule 2 (b) provides some accountability on the part of investigating (authorised) officers in the course of their duty. Surprisingly, there is no cross reference in the CMA to these procedural safeguards in the Police Act, that arguably guarantee (to some extent) the protection of the rights and interests of persons subjected to searches and seizures during police investigations.

The class will then be exposed to the practices in other jurisdictions on the complexities of balancing the competing needs of privacy and law enforcement in computer misuse offences. For instance, in *United States v. Tamura* (1982) the government seized boxes of documents and took them for re-assessment. Some of the documents were evidence of crime mixed with several innocuous documents. Nonetheless, all the documents were seized because it would have been extremely difficult to search through all the boxes on the site. The presiding judge- Betty Fletcher, approved the seizure but suggested that in future the government could "generally avoid fourth amendment rights" in cases involving mingled documents by seeking permission before hand to seize all the documents and conduct an offsite search. That way the "wholesale removal" is "monitored by the judgment of a neutral, detached magistrate." This decision highlights some of the questions that remain regarding the ability of a court to ensure that such judicial approval of the wholesale seizure does not infringe the rights of third parties whose innocuous documents are seized and subjected to scrutiny (Kerr, 2005: pp. 571-576).

The discussion will then turn to responsibilities that are mentioned in Section 28(7) CMA. The section creates an offence for any person to obstruct, hinder or threaten an authorised officer in the performance of their duty or the exercise of his or her powers under the CMA. This responsibility appears to draw parallels with duties of a citizen set out in Objective XXIX (g) of Uganda's Constitution on the duty to uphold and defend the constitution and the law. This Objective denotes that a citizen is obliged to help the police as part of their duty to uphold the law. Notably, responsibilities in Section 28 (7) CMA appears to relate only to individuals under investigation, while Section 28 (7) covers responsibilities of authorised officers.

There is a need to balance police requirements with the rights and responsibilities discussed above, through judicial oversight. Judicial control under the CMA falls to Magistrates Grade I and Chief Magistrates (Section 31). No specific provision exists wherein a magistrate may exercise judicial oversight over the protection of

rights and interests in investigative procedures. The CMA does nevertheless place what appear to be reasonable restrictions, on the execution of a warrant by the authorised officer. Under Section 28 (8), where a computer system or copies of data are seized, they must be returned within 72 hours unless the authorised officer applies for an extension of time. This section does not specify to whom the officer may apply for an extension of time, or the grounds on which such application may be made. Still, if Section 28 (8) is read in conjunction with Section 31, it appears that applications for extension of time may be made before a Magistrate Grade 1 or Chief Magistrate. This implies some measure of judicial oversight.

Finally, it should be noted that Part III of the CMA (Investigations and Procedures) also provides for judicial oversight in unambiguous terms. An investigative officer must apply to court for a Preservation Order to expeditiously preserve data on a computer where there is a belief that data is vulnerable to loss or modification (Section 9). The court must also give judicial approval for an order of disclosure of preserved data and sufficient data to identify service providers under Section 10. Additionally, where the disclosure of data is required for investigation or prosecution, the investigating officer may apply to court for an order compelling a person to submit specified data or for a service provider to submit subscriber information (Section 11). Thus the CMA embraces other aspects of proportionality as set out in the ITU toolkit (Title 3: ***Procedural Provisions for Criminal Investigations and Proceedings for Offenses within this Law*, Sections 14-20).** Ultimately, Sections 9-11 of CMA aim to prevent arbitrary use of procedural powers by the police in the conduct of investigations so as to protect the rights and interests of suspects and third parties.

This progress is laudable given the fact that the procedural framework of the CMA was developed against the backdrop of the narrow context of Uganda's existing criminal procedure legislation (Criminal Procedure Code and the Magistrates Courts Act) that originates from the 1930's old English Assize courts' framework (Owor, 2009: 245-248). These antiquated laws exclude the principle of proportionality and human rights, and judicial oversight. Accordingly, the text of the CMA adequately reflects the proposals of the ULRC that civil liberties, privacy and confidentiality in searches and seizures should be balanced with the need for effective administration of justice. (ULRC Report: paragraph 5.8.1).

Conclusion

To conclude, this paper examined the justifications for teaching of cybercrime on the Bar course. Cybercrime is a nascent area of criminal practice with international dimensions. There is incontrovertible evidence of its existence, and of a fledgling legal framework in place in Uganda. We then critically assessed two legal issues that will predictably arise in scholarly discussions on cybercrime. These are: narrow definitions of cybercrime and procedural concerns of proportionality and human rights, and judicial oversight. The author suggests that the gaps identified in the

CMA could be addressed by LDC in two ways: through research and training of the law teachers. Both modes are the corollary of teaching.

First, LDC has a statutory duty to conduct research under the Law Development Centre Act (Cap 132). Under Section 3 (h), LDC should assist the ULRC in the performance of its functions (of reform and revision of the law). LDC is also enjoined under Section 3 (i) to conduct research into any branch of law. Adopting a multi-faceted approach, the department could conduct research into Uganda's developing cybercrime legislation through socio-legal and doctrinal studies. The findings may be published in peer reviewed journals including LDC's very own *Uganda Law Focus*; and presented at conferences or seminars. That way, building on the student's deliberations, the research department could help reform the law to fit into the international milieu.

Second, at the launch of the ACCP, Dr. Maicibi, the Research and Policy Development Adviser of UNAFRI, informed participants of the ACCP's mission to undertake training of academics in areas such as cyberspace law and cybercrime legislation. Such training is in line with a recommendation that a global understanding of legal issues related to information communication technologies and misuses is of utmost importance (Schjølberg and Ghernaouti-Hélie: p 16). The ACCP's plans as outlined above are a step in the right direction.

LDC is taking measures to prepare for the teaching of cybercrime. The Criminal Proceedings unit is presently reviewing its subject content in such a way as to include case files on cybercrime. Even so, the author accentuates the need for training law teachers in the modern computerised methods of teaching and learning to enable them impart knowledge to their students effectively using electronic media.

Of equal importance is the fact that not all universities will teach cybercrime for their undergraduate Law degrees. This means that LDC must design its Criminal Proceedings course in such a way as to facilitate the teaching of nascent topics such as cybercrime. One way is to teach the subject matter in two parts; the elementary stage (compulsory) and the advanced stage (optional). The latter stage will be for those students who wish to specialise in handling cybercrime cases. Such a proposal to offer optional subjects at LDC was made at the workshop on improving Legal Education in Uganda hosted by LDC (Kampala, November 23, 2010). Although the suggestion was rejected, perhaps now is the time - during the ongoing Bar Course curriculum review - for this proposal to be revisited.

In the meantime, the legal complexities raised in this paper should be investigated by LDC's Department of Research, Law Reform and Publications in collaboration with the newly established ACCP. Ultimately, enriched methods of teaching, research and training of the trainers ought to positively influence LDC's contribution to the development of Uganda's emergent cybercrime legislation.

References

Advocates (*Professional Requirements for Admission to Post Graduate Bar Course*) Legal Notice 17 of 2007
Anti-Terrorism Act (14 of 2002), Laws of Uganda
Candia S. (2010, July 19). Photos of suicide bombers released. *New Vision*, p. 2.
Chawki M and Okike E. (2009) Fighting Cybercrime: Issues for the future. *African Journal of Crime and Criminal Justice,1(1)* 143-175.
Computer Misuse Act (2011)
Constitution of Uganda Chapter 1, Laws of Uganda (2000) as amended by the Constitution (Amendment) Act No. 11/2005 and the Constitution (Amendment) (No. 2) Act 21/2005
Council of Europe *Convention on the prevention of Terrorism* (2005) Warsaw, 16.V.2005
Council of Europe, *Convention on Cybercrime* (2001) Budapest, 23.XI.2001.
Criminal Procedure Code Act, Chapter 116, Laws of Uganda (2000)
*DPP v Bignell [1998]*Criminal Appeal Reports 1
Kisambira E., (May 24, 2010). East Africa to fight cybercrime with CERT. *Computer World Uganda*retrieved from http://news.idg.no/cw/art.cfm?id=CBB60BB2-1A64-6A71-CEB17DB32C209CD3, accessed on July 10, 2010
Electronic Signatures Act 7 of 2011
Electronic Transactions Act 8 of 2011
International Telecommunications Union, (February 2010). Toolkit for cybercrime legislation retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf, accessed on 13th August 2010
Law Development Centre Act Chapter 132, Laws of Uganda (2000)
Law Development Centre.(2009-2010). *Law Development Centre Prospectus* (Kampala, Uganda).
Magistrates Courts Act Chapter 16, Laws of Uganda (2000)
Nanteza, W and Ninsiima, R.(2010, August 3). Cyber law to fight information misuse.*New Vision* retrieved from: http://www.newvision.co.ug/D/8/13/727796, accessed on August 5, 2010
Orin, S. Kerr. (2002). Searches and Seizures In A Digital World. *Harvard Law Review, 119*, 531-585
Owor, M. (2009) *Making International Sentencing Relevant in the Domestic Context: Lessons from Uganda*, Bristol: University of Bristol, Unpublished PhD Thesis.
Police Act Chapter 303 as amended by the Police Amendment Act, Act 16 of 2006
Regina v. Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America H L [1999] ALL ER 1
R vs. Robert and another [1969] East African Law Reports 622
Sita, M. (2010). Welcome Address delivered on August 26, 2010 at UNAFRI, Kampala.
Schjølberg, S and Ghernaouti-Hélie, S. (2009) *A Global Protocol on Cybersecurity and Cybercrime:An initiative for peace and security in cyberspace*retrieved from http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_

and_Cybercrime.pdf, accessed on August 10, 2010.
Senyonjo, M. (2002-2003). Understanding the Right to Privacy as a fundamental human right. *The Uganda Law Focus,* 32-68.
Tushabe F. and Baryamureeba V. (2005). Cyber Crime in Uganda: Myth or Reality? *World Academy of Science, Engineering and Technology*, 8, 66-70.
Uganda Law Reform Commission, *A Study on Electronic Transactions Law* (2006) at: http://www.ulrc.go.ug/reps&pubs/studyReps/Electronic%20Transactions%20Law%20body.pdf, accessed on 10th November 2010
United Nations *Convention against Transnational Organised Crime,* General Assembly Resolution 55/25 of November 15, 2000, entered into force on 29 September 2003
United States v. Tamura 694 F. 2d 591 (9th Cir. 1982)
Walker, C. (2006). Cyber-Terrorism: Legal Principle and Law in the United Kingdom. *Penn State Law Review,(3),* 623-665.

About the author

Maureen Owor, a lawyer, holds the following qualifications: LLB (Hons), Makerere, LLM (Bristol) and PhD (Law), Bristol, England. She is Associate Principal Lecturer and acting Head of the Research, Law Reform and Publications Department at Law Development Centre, Uganda. Maureen also teaches Criminal Proceedings on the Post-graduate Bar Course where she is the Deputy Head of Criminal Proceedings Unit. Maureen is a consultant on the National Taskforce on Sentencing Guidelines. Dr. Owor has previously worked as a State Attorney in the Directorate of Public Prosecutions, a criminal defence lawyer, and Assistant lecturer in Crime, Justice and Society at the University of Bristol. She is a frequent presenter at UNAFRI workshops. Maureen's research areas include: Traditional African courts, Restorative justice, Domestication of international criminal justice and Sentencing in national and international regimes.

The author is indebted to Professor Joseph M. N. Kakooza for his insightful comments.

The Author's personal interests include Badminton, nature walks and singing.

E-mail: mhowor@gmail.com
Cell: +256 (0)791 664 513